UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/017,392	12/18/2001	Yuusaku Ohta	2001_1828A	6503

513 7590 05/16/2005

WENDEROTH, LIND & PONACK, L.L.P.
2033 K STREET N. W.
SUITE 800
WASHINGTON, DC 20006-1021

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 05/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/017,392	**Applicant(s)** OHTA ET AL.	
	Examiner Tamara Teslovich	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _18 December 2001_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-19_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-19_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _18 December 2001_ is/are: a)□ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _10.15.02 12.18.01_.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Drawings

Figure 1 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

Claims 1, 2, 6, 11, 13, and 15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "inputted packet" in page 51, line 26. There is insufficient antecedent basis for this limitation in the claim.

Claim 2 recites the limitation "the first type packet" in line 1, "the second type packet" in line 2, "the third type data packet" in line 4, and "the fourth type data packet" in line 6 of page 52. There is insufficient antecedent basis for these limitations in the claim.

Claim 6 recites the limitation "the first type packet" in line 25, “the second type packet” in line 26, “the third type data packet” in line 28, and “the fourth type data packet” in line 30 of page 53. There is insufficient antecedent basis for these limitations in the claim.

Claim 11 recites the limitation “the data path connection switching unit” in line 28 of page 55. There is insufficient antecedent basis for this limitation.

Claim 13 recites the limitation “the processing data saving unit” in line 15 of page 56. There is insufficient antecedent basis for this limitation.

Claim 15 recites the limitation “the data path connection switching unit” in line 1 of page 57. There is insufficient antecedent basis for this limitation.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 2, 5, 6, 9, 13, and 17-10 are rejected under 35 U.S.C. 102(e) as being anticipated by Donald P. Matthews (U.S. Patent Application Publication 2002/0078342).

As per claim 1, Matthews discloses a security communication packet processing apparatus that performs at least one of encryption processing, decryption processing and authentication processing to a packet comprising:

one or more encryption processing unit ("cryptography engine") operable to perform the encryption processing and the decryption processing in a data block unit of B1 bits (Matthews [0031]);

one or more authentication processing units ("authentication engine") operable to perform the authentication processing in a data block unit of B2 (= n x B1) bits in parallel to the encryption processing or the decryption processing by the encryption processing unit, and output an authentication value indicating the result of the authentication processing (Matthews [0029]);

one or more data block accumulation unit ("authentication alignment block") operable to accumulate the data blocks to which the encryption processing is performed by the encryption processing unit, and, when the accumulated amount of the data blocks reaches B2 bits, output the data blocks to the authentication processing unit (Matthews [0027]);

a packet construction unit operable to receive the encrypted or decrypted data blocks from the encryption processing unit, receive the authentication value from the authentication processing unit, and construct a packet including the received data blocks and authentication value (Matthews [0026]); and a control unit operable ("cryptography alignment block") to divide the inputted packet into the data blocks of B1 bits, and output the data blocks sequentially to the encryption processing unit (Matthews [0031]).

As per claim 2, Matthews discloses the security communication packet processing apparatus according to Claim 1, wherein the control unit judges which type the inputted packet is, the first type packet requiring the encryption processing and the authentication processing, the second type packet requiring the decryption processing and the authentication processing, the third type packet requiring one of the encryption processing and the decryption processing, or the fourth type packet requiring the authentication processing only (Matthews [0011] reference 'distinguishes portions of non-pre-padded network security protocol packet requiring one and/or another operation - authentication and/or encryption" to permit single pass processing of data),

when the packet is judged to be the first type packet, divides the packet into the data blocks of B1 bits and outputs the data blocks sequentially to the encryption processing unit (Matthews [0031]),

when the packet is judged to be the second type packet, divides the packet into the data blocks of B1 bits, outputs them sequentially to the encryption processing unit (Matthews [0031]), divides the packet or the duplicate of the packet into the data blocks of B2 bits, and outputs the data blocks sequentially to the authentication processing unit (Matthews [0027]), when the packet is judged to be the third type packet, divides the packet into the data blocks of B1 bits and outputs the data blocks sequentially to the encryption processing unit (Matthews [0031]), and

when the packet is judged to be the fourth type packet, divides the packet into the data blocks of B2 bits and outputs the data blocks sequentially to the authentication processing unit (Matthews [0027]).

As per claim 5, Matthews discloses the security communication packet processing apparatus according to Claim 1 further comprising:

a data path connection switching unit ("alignment logic configuration") that can connect the output of the control unit and the input of the encryption processing unit, the output of the control unit and the input of the authentication processing unit, the output of the encryption processing unit and the input of the data block accumulation unit, and the output of the data block accumulation unit and the input of the authentication processing unit, respectively and independently (Matthews [0024]).

As per claim 6, Matthews discloses the security communication packet processing apparatus according to Claim 5,

wherein the control unit judges which type the inputted packet is, the first type packet requiring the encryption processing and the authentication processing, the second type packet requiring the decryption processing and the authentication processing, the third type packet requiring one of the encryption processing and the decryption processing, or the fourth type packet requiring the authentication processing only (Matthews [0011] reference ‘distinguishes portions of non-pre-padded network security protocol packet requiring one and/or another operation - authentication and/or encryption” to permit single pass processing of data),

when the packet is judged to be the first type packet, controls the data path connection switching unit so as to connect the output of the control unit and the input of the encryption processing unit, the output of the encryption processing unit and the input of the data block accumulation unit, and the output of the data block accumulation unit and the input of the authentication unit (Matthews [0031]),

when the packet is judged to be the second type packet, controls the data path connection switching unit so as to connect the output of the control unit and the input of the 10 encryption processing unit, and the output of the control unit and the input of the authentication unit (Matthews [0027]),

when the packet is judged to be the third type packet, controls the data path connection switching unit so as to connect the output of the control unit and the input of the encryption processing unit (Matthews [0031]),

when the packet is judged to be the fourth type packet, controls the data path connection switching unit so as to connect the output of the control unit and the input of the authentication processing unit (Matthews [0027]).

As per claim 9, Matthews discloses the security communication packet processing apparatus according to Claim 1 further comprising:

a processing data saving ("memory") unit, for each of at least one of the encryption processing unit, the authentication processing unit and the data block accumulation unit, that has a memory area for temporarily saving the data blocks which are being processed in the processing unit corresponding respectively to the processing unit (Matthews [0032]).

As per claim 13, Matthews discloses the security communication packet processing apparatus according to Claim 1 further comprising: a processing data saving ("memory") unit, for each of at least two of the encryption processing unit, the authentication processing unit and the data block accumulation unit, that has a memory area shared by the processing units for temporarily saving the data blocks which are being processed in the processing units (Matthews [0032]).

As per claim 17, Matthews discloses the security communication packet processing apparatus according to claim 1,

wherein the B1 is 64 (Matthews [0027]), and

the B2 is 512 (Matthews [0029]).

As per claim 18, Matthews discloses a security communication packet processing method that performs at least one of the encryption processing, decryption processing and the authentication processing to the packet including:

a dividing step for dividing the inputted packet into the data blocks of B1 bits (Matthews [0031]);

an encryption processing step for performing the encryption processing or the decryption processing to the divided data blocks of B1 bits (Matthews [0031]);

a data block accumulating step for accumulating the encrypted data blocks and outputting the data blocks when the accumulated amount of the data blocks reaches B2 (= n x B1) bits (Matthews [0027]);

an authentication processing step for performing the authentication processing to the outputted data blocks of B2 bits in parallel to the encryption processing or the decryption processing, and outputting the authentication value indicating the result of the authentication processing (Matthews [0029]);

a packet constructing step for receiving the encrypted or decrypted data blocks, receiving the authentication value, and constructing the packet including the received data blocks and authentication value (Matthews [0026]).

As per claim 19, Matthews discloses the security communication packet processing method according to claim 18 further including:

a control step for judging which type the inputted packet is the first type packet requiring the encryption processing and the authentication processing, the second type packet requiring the decryption processing and the authentication processing, the third type packet requiring only one of the encryption processing and the decryption processing, or the fourth type packet requiring the authentication processing only, and when it is judged to be the first type packet, controlling so that the division in the dividing step, the encryption processing in the encryption processing step, the accumulation in the data block accumulating step, the authentication processing in the authentication processing step and the construction in the packet constructing step are performed (Matthews [0011] reference 'distinguishes portions of non-pre-padded network security protocol packet requiring one and/or another operation - authentication and/or encryption" to permit single pass processing of data).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3, 4, 7, 8, 10-12, and 14-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matthews as applied to claims 1, 2, 5, 6, 9, 13, and 17-19 above, and further in view of Videcrantz et al. (U.S. Patent No. 6,275,588).

As per claim 3, Matthews discloses the security communication packet processing apparatus according to Claim 1.

Matthews fails to teach wherein the number of at least one of the encryption processing unit and the authentication unit is two or more, and the number of the data block accumulation unit is equal to that of the encryption processing unit.

Videcrantz discloses a security communication packet processing apparatus including a plurality of encryption processing units and authentication processing units wherein the number of accumulation units is equal to that of the encryption processing units (see Figure 11b).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Matthews the plurality of units as described in Videcrantz to remove queuing delays resulting from a plurality of packets attempting to utilize the units at the same time.

As per claim 4, Matthews discloses the security communication packet processing apparatus according to Claim 3.

Matthews fails to teach wherein the control unit specifies, among two or more encryption processing units or two or more authentication processing units, the encryption processing unit or the authentication processing unit that is ready for processing, and outputs the data blocks to the specified encryption processing unit or the authentication processing unit.

Videcrantz discloses a security communication packet processing apparatus including a plurality of processing units and authentication units wherein the control unit specifies which processing unit is to be utilized (see Figure 11b).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Matthews a control unit with the capabilities to determine which processing units have completed their calculations and are ready to output to the next processing unit as described in Videcrantz to in order to maintain order and expedite the time necessary to deal with incoming packets.

As per claim 7, Matthews discloses the security communication packet processing apparatus according to Claim 6.

Matthews fails to teach wherein the number of at least one of the encryption processing unit and the authentication unit is two or more, and the number of the data block accumulation unit is equal to that of the encryption processing unit.

Videcrantz discloses a security communication packet processing apparatus including a plurality of encryption processing units and authentication processing units wherein the number of accumulation units is equal to that of the encryption processing units (see Figure 11b).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Matthews the plurality of units as described in Videcrantz to remove queuing delays resulting from a plurality of packets attempting to utilize the units at the same time.

As per claim 8, Matthews discloses the security communication packet processing apparatus according to Claim 7.

Matthews fails to teach wherein the control unit specifies, among two or more encryption processing units or two or more authentication processing units, the encryption processing unit or the authentication processing unit that is ready for processing, and outputs the data blocks to the specified encryption processing unit or the authentication processing unit.

Videcrantz discloses a security communication packet processing apparatus including a plurality of processing units and authentication units wherein the control unit specifies which processing unit is to be utilized (see Figure 11b).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Matthews a control unit with the capabilities to determine which processing units have completed their calculations and are ready to output to the next processing unit as described in Videcrantz to in order to maintain order and expedite the time necessary to deal with incoming packets.

As per claim 10, Matthews discloses the security communication packet processing apparatus according to claim 9,

wherein the control unit specifies the processing unit that is performing the processing of the data blocks of the packet with the lowest priority among the processing units, and after saving the data blocks which are being processed in the processing unit into the processing data saving unit, makes the processing unit perform the processing of the data blocks of the inputted packet (Matthews [0035]).

As per claim 11, the combined apparatus of Matthews and Videcrantz discloses the security communication packet processing apparatus according to Claim 10 further comprising:

a data path connection switching unit that can connect the output of the control unit and the input of the encryption processing unit, the output of the control unit and the input of the authentication processing unit, the output of the encryption processing unit and the input of the data block accumulation unit, and the output of the data block accumulation unit and the input of the authentication processing unit, respectively and independently (Matthews [0024]).

As per claim 12, Matthews discloses the security communication packet processing apparatus according to Claim 11.

Matthews fails to teach wherein the number of at least one of the encryption processing unit and the authentication unit is two or more, and the number of the data block accumulation unit is equal to that of the encryption processing unit.

Videcrantz discloses a security communication including a plurality of encryption processing units and authentication processing units wherein the number of accumulation units is equal to that of the encryption processing units (see Figure 11b).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Matthews the plurality of units as described in Videcrantz to remove queuing delays resulting from a plurality of packets attempting to utilize the units at the same time.

As per claim 14, Matthews discloses the security communication packet processing apparatus according to Claim 13, wherein the control unit specifies, among the processing units, the processing unit that is performing the processing of the data blocks of the packet with the lowest priority, and after saving the data blocks which are being processed in the processing unit in the processing data saving unit, makes the processing unit perform the processing of the data blocks of the inputted packet (Matthews [0035]).

As per claim 15, the combined apparatus of Matthews and Videcrantz discloses the security communication packet processing apparatus according to Claim 14 further comprising:

a connection switching unit that can connect control unit and the input of the encryption processing unit, the output of the control unit and the input of the authentication processing unit, the output of the encryption processing unit and the input of the data block accumulation unit, and the output of the data block accumulation unit and the input of the authentication processing unit, respectively and independently (Matthews [0024]).

As per claim 16, Matthews discloses the security communication packet processing apparatus according to Claim 15.

Matthews fails to teach wherein the number of at least one of the encryption processing unit and the authentication unit is two or more, and the number of the data block accumulation unit is equal to that of the encryption processing unit.

Videcrantz discloses a security communication packet processing apparatus including a plurality of encryption processing units and authentication processing units wherein the number of accumulation units is equal to that of the encryption processing units (see Figure 11b).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Matthews the plurality of units as described in Videcrantz to remove queuing delays resulting from a plurality of packets attempting to utilize the units at the same time.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

T. Teslovich
May 5, 2005